



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/870,610	05/31/2001	Dwip N. Banerjee	AUS9-2001-0361-US1	1787

40412 7590 03/03/2006

IBM CORPORATION- AUSTIN (JVL)
C/O VAN LEEUWEN & VAN LEEUWEN
PO BOX 90609
AUSTIN, TX 78709-0609

EXAMINER

BAYARD, DJENANE M

ART UNIT PAPER NUMBER

2141

DATE MAILED: 03/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/870,610	Applicant(s) BANERJEE ET AL.	
	Examiner Djenane M. Bayard	Art Unit 2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 December 2005.
 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1, 5, 8, 11, 14, 18 and 21-30 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) ☐ Claim(s) _____ is/are allowed.
 6) ☒ Claim(s) 1, 5, 8, 11, 14, 18 and 21-30 is/are rejected.
 7) ☐ Claim(s) _____ is/are objected to.
 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
 10) ☒ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☐ All b) ☐ Some * c) ☐ None of:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response to amendment filed on 12/16/05 in which claims 1, 5, 8, 11, , 14, 18, 21-30 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1, 5, 8, 11, 14, 18, 21-26 and 28-30 have been considered but are moot in view of the new ground(s) of rejection.

3. As per claim 27, Applicant argues Ptacek never teaches or suggests adjusting a server configuration setting based on the analysis, wherein the adjusted server configuration setting is selected from group consisting of the stored packet limit and the stored socket limit. However, Ptacek clearly teaches wherein the CASL is intended simulate attacks against host in order to see if those hosts are vulnerable to attacks of a given nature (See col. 6, lines 29-53). Furthermore, Ptacek teaches wherein one of those simulated attacks will actually send connection requests to each reserved ports (See col. 26, lines 25-37). It would have been obvious to one with ordinary skill in the art to conclude that Ptacek is doing simulated network attack in order to test the vulnerabilities of the network and to adjust the configuration setting.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1, 5, 8, 11, 14, 18 and 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2003/0110396 to Lewis et al in view of U.S. Patent No. 6,189,035 to Lockhart et al.

a. As per claims 1, 8 and 14, Lewis et al teaches a method and apparatus for predicting and preventing attacks in communication networks. Furthermore, Lewis et al teaches providing a test script, the test script including one or more attack simulations (See page 5, paragraph [0061], *the Master infiltrates multiple computer systems and installs the Ddos tools, which are scripts capable of generating large volumes of traffic*) ; processing the attack simulations included in the test script (See page 5, paragraph [0062]) ; determining whether to change one or more configuration settings based upon the processing (See page 2, paragraph [0018], *one or more of the triggers signal the action-taking means to take the appropriate protective action*) ; changing one or more of the configuration settings based upon determination (See page 2, paragraph [0020], *the protective action are therefore automatically undertaken by the management system*); However, Lewis et al fails to teach receiving a packet from a client computer; identifying the client computer by a source Ip address; calculating a number of packets received using the source Ip address during a time interval, wherein the calculating includes Retrieving a number of packets received that correspond to the source Ip address; and incrementing the number of packets received; comparing the incrementing number of packets received with one or more

Art Unit: 2141

configuration settings; determining an action from a plurality of actions based on the comparing; and executing the action.

Lockhart et al teaches a method for protecting a network from data packet overload. Furthermore, Lockhart et al teaches identifying the client computer by a source Ip address (See col. 3, lines 25-26, *a determination is made as to whether the incoming data packet has an IP address that is stored in the table*) ; calculating a number of packets received using the source Ip address during a time interval, wherein the calculating includes retrieving a number of packets received that correspond to the source Ip address (See col. 3, lines 65-67 and col. 4, lines 1-50, *a recent packet count is maintained for each IP source that sends data packets to the internal network during a most recent cycle, where a cycle is a time period of several minutes or hours during which the gate 20 receives incoming data packets*); incrementing the number of packets received (See col. 4, lines 3-4, that recent packet count for the present IP source is incremented by one); comparing the incrementing number of packets received with one or more configuration settings (See col. 4, lines 14-21, *a determination is made as to whether the recent packet count for this particular IP source exceeds a predetermined threshold*) ; determining an action from a plurality of actions based on the comparing; and executing the action (See col. 4, lines 14-26, *if the answer is affirmative, the process advances to where the data packet is discarded ...*).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate the teaching of Lockhart et al in the claimed invention of Lewis et al in order for the number of incoming data packets that are passed to the internal network be limited to a number which the internal network can handle without unduly degrading its operation (See col. 2, lines 51-56).

b. As per claims 5, 11 and 18, Lewis et al in view of Lockhart et al teaches the claimed invention as described above. However, Lewis et al in view of Lockhart et al fails to teach receiving a socket request from the client computer; determining a number of sockets opened for the client computer; comparing the number of sockets opened to a socket limit; and determining whether to allow a socket request based on the comparison.

Goldstone teaches prevention of bandwidth congestion in a denial of service or other internet-based attack. Furthermore, Godlstone teaches receiving a socket request from the client computer; determining a number of sockets opened for the client computer; comparing the number of sockets opened to a socket limit; and determining whether to allow a socket request based on the comparison (See page 3, paragraph [0038]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate receiving a socket request from the client computer; determining a number of sockets opened for the client computer; comparing the number of sockets opened to a socket limit; and determining whether to allow a socket request based on the comparison as taught by Goldstone in the claimed invention of Lewis et al in view of Lockhart et al in order for the router to prevent the attacking client from perpetrating further attacks by blocking traffic originating from the attacking client from entering the Internet (See page 3, paragraph [0027]).

c. As per claims 28, 29 and 30, Lewis et al in view of Lockhart et al teaches the claimed invention as described above. Furthermore, Lewis et al teaches wherein at least one of the

Art Unit: 2141

configuration settings are selected from the group consisting of a number of packets allowed, a time interval, a server port, and an overcount action (See page 4, paragraph [0050]).

5. Claims 21, 23 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2003/0110396 to Lewis et al in view of U.S. Patent No. 6,189,035 to Lockhart et al as applied to claim 1, 8 and 16 above and further in view of U.S. Patent No. 6,381,649 to Carlson.

a. As per claim 21, 23 and 25, Lewis et al in view of Lockhart et al teaches the claimed invention as described above. However, Lewis et al in view of Lockhart et al fails to teach wherein configuration settings include a first limit and a second limit, the method further comprising: determining that the incremented number of packets exceeds the first limit; processing the packet and sending a notification in response to determining the incremented number of packets exceeds the first limit; receiving a subsequent packet from the client computer; incrementing again the number of packets in response to receiving the subsequent packet; determining that the incremented again number of packets exceeds the second limit; and rejecting the subsequent packet in response to determining that the incremented again number of packets exceeds the second limit.

Carlson et al teaches determining that the number of packets exceeds the first limit; sending a notification in response to determining the number of packets exceeds the first limit; receiving a subsequent packet from the client computer; incrementing the number of packets in response to receiving the subsequent packet; determining that the incremented number of packets

Art Unit: 2141

exceeds the second limit; and rejecting the subsequent packet in response to determining that the incremented number of packets exceeds the second limit (See col. 7, lines 55-67 and col. 8, lines 1-8).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate determining that the number of packets exceeds the first limit; sending a notification in response to determining the number of packets exceeds the first limit; receiving a subsequent packet from the client computer; incrementing the number of packets in response to receiving the subsequent packet; determining that the incremented number of packets exceeds the second limit; and rejecting the subsequent packet in response to determining that the incremented number of packets exceeds the second limit as taught by Carlson in the claimed invention of Lewis et al in view of Lockhart et al in order to monitor or police data traffic 9See col. 1, lines 61-64).

6. Claims 22, 24 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application No. 2003/0110396 to Lewis et al in view of U.S. Patent No. 6,189,035 to Lockhart et al as applied to claim 1, 8 and 16 above and further in view of U.S. Patent No. 6,321,338 Porras et al.

a. As per claim 22, 24 and 26, Lewis et al in view of Lockhart et al teaches the claimed invention as described above. However, Lewis et al in view of Lockhart et al fails to teach wherein the configuration settings include a historical' usage corresponding to the client computer, the method further comprising: determining that the number of packets is higher than

Art Unit: 2141

the historical usage; and sending a notification in response to determining that the number of packets is higher than the historical usage.

Porras et al teaches wherein the configuration settings include a historical' usage corresponding to the client computer, the method further comprising: determining that the number of packets is higher than the historical usage (See col. 6 and 7); and sending a notification in response to determining that the number of packets is higher than the historical usage (See col. 2, lines 54-56).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate wherein the configuration settings include a historical' usage corresponding to the client computer, the method further comprising: determining that the number of packets is higher than the historical usage; and sending a notification in response to determining that the number of packets is higher than the historical usage as taught by Porras et al in the claimed invention of Gupta et al in view of Goldstone and further in view of Lockhart et al in order to identify attacks causing disturbances in more than one network entity 9See col. 2, lines 58-60).

7. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,636,972 to Ptacek et al in view of U.S. Patent No. 6,189,035 to Lockhart et al and further in view of U.S. Patent Application No. 2002/0059454 to Barrett et al.

a. As per claim 27, Ptacek et al teaches a system and method for building an executable script for performing a network security audit. Furthermore, Ptacek et al teaches executing a test

Art Unit: 2141

script that includes one or more attack simulations from the client computer, the execution of the test script including (See col. 24, lines 30-42): receiving, at the server computer, one or more packets from the client computer and one or more open socket requests from the client computer (See col. 26, lines 25-37) and the evaluating including: analyzing the performance of the server computer during the simulation; and adjusting a server configuration setting based on the analysis, wherein the adjusted server configuration setting is selected from a group consisting the stored packet limit and the stored socket limit (See col. 6, lines 29-53). However, Ptacek et al fails to teach deciding a packet threshold for the client computer the deciding including: determining a number of packets received from the client computer during a time interval; incrementing the number of packets received from the client computer; and comparing the number of packets received with a packet limit stored at the server computer; computing an open socket threshold for the client computer, the computing including: determining a number of opened sockets for the client computer; incrementing the number of opened sockets for the client computer; comparing the number of sockets opened for the client computer to a socket limit stored at the server computer; and evaluating the packet limit and the socket limit used during the attack simulations.

Lockhart et al teaches a recent packet count is maintained for each IP source that sends data packets to the internal network during a most recent cycle, where a cycle is a time period of several minutes or hours during which the gate 20 receives incoming data packets. In the next step 60, that recent packet count for the present IP source is incremented by one. (18). The present process also maintains a count representing the count of all data packets received... If the answer is negative, the program proceeds to step 70 where a determination is made as to whether

the total packet count exceeds its threshold. If the answer is negative, the packet is negative. Otherwise, the packet is discarded. (See col. 3, lines 65-67 and col. 4, lines 1-50).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate deciding a packet threshold for the client computer the deciding including: determining a number of packets received from the client computer during a time interval; incrementing the number of packets received from the client computer; and comparing the number of packets received with a packet limit stored at the server computer as taught by Lockhart et al in the claimed invention of Ptacek et al in order to determine the packet loss rate calculation over a predetermined window interval (See col. 21, lines 65-67). However, Ptacek et al in view of Lockhart et al fails to teach: determining a number of opened sockets for the client computer; incrementing the number of opened sockets for the client computer; comparing the number of sockets opened for the client computer to a socket limit stored at the server computer; and evaluating the packet limit and the socket limit used during the attack simulations.

Barrett et al teaches determining a number of opened sockets for the client computer; incrementing the number of opened sockets for the client computer; comparing the number of sockets opened for the client computer to a socket limit stored at the server computer; and evaluating the packet limit and the socket limit used during the attack simulations (See page 1, paragraph [0006]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate determining a number of opened sockets for the client computer; incrementing the number of opened sockets for the client computer; comparing the number of sockets opened for the client computer to a socket limit stored at the server computer; and

Art Unit: 2141

evaluating the packet limit and the socket limit used during the attack simulations as taught by Barrett et al in the claimed invention of Ptacek et al in view of Lockhart et al in order to limit to a number which the internal network can handle the number of incoming packet without unduly degrading its operation (See col. 2, lines 51-56).

Conclusion

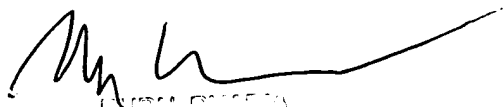
8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Djenane M. Bayard whose telephone number is (571) 272-3878. The examiner can normally be reached on Monday- Friday 5:30 AM- 3:00 PM..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Djenane Bayard

Patent Examiner



INSTITUTION
SUPERVISORY PATENT EXAMINER